NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE EFFECTS OF DISRUPTIVE TECHNOLOGY ON PROJECT INTERDICTION

by

Timothy L. Adduce

December 2016

Thesis Advisor: W. Matthew Carlyle
Second Reader: Gerald Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE THE EFFECTS OF DISRUPTIVE TECHNOLOGY ON PROJECT INTERDICTION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Timothy L. Adduce	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

We model a project network that uses common methods of improvised explosives and metallic liner manufacture for the purposes of constructing anti-armor IEDs. Separately, we model a network utilizing advanced 3D printing technology for the same ends. We then introduce an interdiction extension to both project models.

By utilizing decision critical path method models, we examine the differences in the critical paths of both project networks. Our finding of note is that the length of the network employing advanced 3D printing technology is significantly shorter, even after the attacker's interdiction efforts. Because the length of the critical path of this network remains significantly shorter, advanced 3D printing technology can be considered to be a "disruptive technology."

This flexible modeling can be rapidly implemented when future technological "black swans" appear. This modeling provides decision makers with clear, quantitative analysis and can be used to drive future intelligence and capability requirements, as well as to inform potential policy responses.

14. SUBJECT TERMS disruptive technology, critical path method, PERT, IED, optimization, defender-attacker	**15. NUMBER OF PAGES** 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE EFFECTS OF DISRUPTIVE TECHNOLOGY ON PROJECT INTERDICTION

Timothy L. Adduce
Lieutenant, United States Navy
B.S., United States Naval Academy, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
December 2016

Approved by: W. Matthew Carlyle
Thesis Advisor

Gerald Brown
Second Reader

Patricia Jacobs
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

We model a project network that uses common methods of improvised explosives and metallic liner manufacture for the purposes of constructing anti-armor IEDs. Separately, we model a network utilizing advanced 3D printing technology for the same ends. We then introduce an interdiction extension to both project models.

By utilizing decision critical path method models, we examine the differences in the critical paths of both project networks. Our finding of note is that the length of the network employing advanced 3D printing technology is significantly shorter, even after the attacker's interdiction efforts. Because the length of the critical path of this network remains significantly shorter, advanced 3D printing technology can be considered to be a "disruptive technology."

This flexible modeling can be rapidly implemented when future technological "black swans" appear. This modeling provides decision makers with clear, quantitative analysis and can be used to drive future intelligence and capability requirements, as well as to inform potential policy responses.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AR	ArmaLite Rifle
ATF	Alcohol Tobacco Firearms
BATFE	Bureau of Alcohol Tobacco Firearms and Explosives
CAD	computer aided design
CHP	Concentrated Hydrogen Peroxide
CPM	critical path method
DIY	Do It Yourself
EFP	Explosively Formed Penetrators
ETN	Erythritol Tetranitrate, a powerful booster explosive
GSE	Government Sponsored Entities
HMTD	Hexamethylene Triperoxide Diamine
HMX	Cyclotetramethylene-tetranitramine, similar to RDX
IED	Improvised Explosive Device
NSA	National Security Agency
PERT	Program Evaluation and Review Technique
RDX	Cyclotrimethlenetrinitramine, a highly brisant explosive
SEC	Solution Elimination Constraint
TATP	Triacetone Triperoxide
TOR	The Onion Router
3D	three-dimensional

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The “black swan” technological development that motivates this particular analysis is the emergence of advanced additive manufacturing, or 3D printing, which is rapidly growing in capability while decreasing in price. We therefore assess the changes in network structure and resiliency that take place when a nefarious actor acquires such technology and uses it to clandestinely produce weapons. We consider advanced 3D printers as a candidate for those technologies that have become known in the popular discourse as “disruptive technologies.” Our objective is to propose a definition for the term “disruptive technology” and illustrate how to quantitatively assess whether or not any given technology fits this definition. We thus introduce a method that utilizes decision critical path method (CPM) models. Decision CPMs are infinitely scalable and rapidly implementable. This makes decision CPMs the ideal tool for assessing technological “black swans” once they emerge.

To illustrate how this process works, we consider two separate project networks. The first utilizes common methods for improvised explosives manufacture and is referred to as the legacy project network. Additionally, we pair these explosives with metallic liners to produce a particular type of improvised explosive device (IED) known as an explosively formed penetrator (EFP). These devices were known for their ability to remain lethal at significant distances and were responsible for many of the casualties suffered in Operation Iraqi Freedom. To produce an effective version of this device without ready access to military explosives of sufficiently high brisance would require a complex series of operations; to safely build such devices in any significant quantity would take a bomb maker of some skill. Repeatedly completing these tasks in the face of an observant adversary, while certainly possible, would likely require considerable time unless the bomb-maker, referred to henceforth as the “operator,” did not consider personal survival a priority.

The second project network utilizes advanced 3D printing, capable of printing complex molecules out of ubiquitous feedstocks, to produce an IED and is referred to as the advanced network. The length of time required for project completion in this network

is noticeably shorter (on the order of 60% less). Additionally, this network is far less susceptible to interdiction efforts undertaken by an attacker and is presumed to require less skill on the part of the bomb maker.

Our decision CPM model, referred to as DISTECH, allows an analyst to utilize standard project management software to model any type of adversary project desired, whether it employs a candidate disruptive technology or not. DISTECH then implements an attacker extension in an effort to maximally delay by interdicting tasks that maximize the length of the resulting critical path. The length of time required to complete a project corresponds to the length of the "critical path." By comparing the differences in the lengths of the post-interdiction critical paths between a legacy project network and an advanced project network employing a candidate disruptive technology, an analyst can determine whether the candidate technology is truly disruptive and make quantitative assessments about the magnitude of the disruption posed. As such, we can now assert that the proper way to address disruptive technologies is not to attempt to predict the future, but rather to rapidly respond in a measured, intelligent fashion. What is more, the DISTECH model introduces a new family of SKIP variables to help assess the cost of interdiction as well as allowing the analysist to model a variety of situations with a single mechanism.

ACKNOWLEDGMENTS

First, I would like to thank my wife for putting up with all of my late-night library excursions. Many thanks are also due to my advisors, especially Professor Carlyle, without whose help I'd still be staring at GAMs error messages.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

When the printing press emerged in the middle of the 15th century, the Catholic Church and ruling nobility could not foresee the consequences such a disruptive technology would have. Mass-produced translations of the Bible in native languages contributed greatly to massive social and political upheavals that would forever change the course of European and world history during the German Peasant's War and the Protestant Reformation, among others. Spreading these alternative interpretations of scripture and their attendant social philosophies was a network of scholars and printers who labored in a loose structure of associations we today might represent as a project network model. If one were to observe this project network both before and after the introduction of the printing press, we would observe that its structure had changed significantly. Producing any given number of texts now required far less expenditure of effort and support and made combating the spread of these ideas all the more difficult. One would observe similar effects today in employing disruptive technologies to develop, for example, improvised weapons.

One cannot plausibly hope to foresee what technological "black swans" will appear in the future. Decision critical path method models can, however, allow one to rapidly assess such effects once a disruptive technology emerges. This in turn can aid decision makers in choosing how to respond to disruptive technologies and those adversaries who employ them. The key to dealing with disruptive technology is therefore not in prediction or in attempting to restrain human technological or social evolution, but rather the rapid adaptation of current security paradigms and procedures to the new realities introduced by disruptive technologies.

Western societies with a robust middle class will likely be the first to experience the effects of disruptive technology. This is true for several reasons. First, Western governments maintain stringent controls on military hardware. Storage requirements, physical security, and regular inventories help ensure military ordnance and related

hardware does not fall into unauthorized hands [1]. Nefarious actors must therefore utilize various illicit or improvised methods to acquire weapons in support of their agendas. These weapons include everything from firearms and explosives to even rudimentary chemical agents. In contrast, countries like Iraq and Afghanistan are already awash in military hardware and the governments struggle to provide basic services and border integrity, let alone maintain accountability for their own equipment. Conditions like these make the adoption of disruptive technologies uneconomical considering how easily conventional munitions can be attained. Therefore, stringent controls provide the incentive to adopt disruptive technologies while higher levels of disposable income provide the means to acquire them in Western societies. Additionally, high levels of education and easy capital formation result in such technologies primarily being developed in liberal democracies. Since these societies tend to be the main developers of such technologies, it stands to reason they will also be the first to experience the consequences, both good and bad.

Future disruptive technologies will likely alter the balance of power very differently than they have in the past. The airplane, a disruptive technology that fundamentally changed the way wars are fought, still requires the vast industrial base of a nation state to produce. It is therefore highly implausible that individuals could produce a capable combat aircraft of their own in any significant quantity. Because of this, the aircraft was disruptive only at the level of competing nation states. Future disruptive technologies will likely alter the balance of power between nations and legacy industries relative to the individual. The capability of individuals to threaten social, economic, and security norms will likely increase due to the highly decentralized and disintermediating nature of powerful new disruptive technologies.

B. DISRUPTIVE TECHNOLOGY IN TODAY'S CONTEXT

The Sandy Hook Elementary School shooting on December 12, 2012, shocked America and ignited a firestorm of debate concerning the nature and extent of current firearm regulations. Proponents of expanded regulation claimed, and still do, that such restrictions are needed in the interest of community safety, while detractors questioned

the efficacy of such restrictions. Meanwhile, Cody Wilson, a 25-year-old former student of the University of Texas School of Law, was fervently working on overcoming the technical challenges associated with 3D printing firearms and firearms components, or so-called “wiki weapons” [2]. Effective wiki weapons would, by design, circumvent any possible regulatory actions. Initially, members of the firearms community had a rather blasé attitude regarding Wilson’s work, but in the wake of Sandy Hook and the renewed support by regulators to ban and/or confiscate high capacity magazines and semi-automatic rifles, interest in Wilson’s work intensified.

Early in 2013, Wilson posted a video to YouTube of himself shooting an AR-15 rifle with a plastic, fully 3D-printed lower receiver. The lower receiver of the AR-15 rifle is considered by the Bureau of Alcohol Tobacco Firearms and Explosives (BATFE) as the functional component that makes the AR-15 a firearm and is thus regulated as such. Early prototypes failed after only a few rounds. Undeterred, the wiki weapon community quickly developed a lower receiver capable of firing over 650 rounds of 5.56mm ammunition, which Wilson himself test fired in a YouTube video in the early spring of 2013. Wilson, however, was not satisfied. He wanted to design and freely distribute a fully 3D printable firearm. On May 6, 2013, the single shot Liberator pistol was posted to Wilson’s online computer aided design (CAD) file repository, DEFDIST.org [2]. In Wilson’s words, it served as a “demonstrative spectacle” of how modern law enforcement and security paradigms could be undermined with relative ease, given current 3D printing technology [3].

Regardless of one’s personal beliefs regarding arms control, one must concede that 3D printing has already begun to upset the regulatory paradigms in place around the world. The Liberator was downloaded more than 100,000 times before the United States Department of State ordered Wilson to take the Liberator CAD file offline, despite the fact that this response came within 24 hours of the initial post. The State Department claimed the design was in fact government property under the Cold-War-vintage International Traffic in Arms Regulations law. Interestingly enough, much of the downloading was completed by persons in regions with much stricter gun control regulations, such as Europe and Asia. Soon afterward, multiple anonymously posted

videos emerged on YouTube from around the world, showcasing individuals firing their Liberator pistols. So, despite the direct intervention of the U.S. State Department and the stringent arms control regulations in place in many foreign countries, novice do-it-yourself (DIY) gunsmiths had succeeded in acquiring for themselves this first generation of wiki weapons [2],[4]. CAD files for high-capacity magazines, AR lower receivers, and the original Liberator pistol and numerous improved repeating firearm designs remain available online in such locations as The Pirate Bay and multiple other file sharing sites. With the ability to turn lines of code into physical objects, these so-called "physible" files are, and are highly likely to remain, outside of the ability of regulators to control.

The plight of regulators and law enforcement is unlikely to improve. Already, desktop printers that print with more rugged materials, like steel and aluminum, are reaching price points that put them within reach of the average handyman. In as little as 25 years, it may well be within the financial means of average citizens to purchase 3D printers capable of assembling complex molecules out of cheap and widely available feedstocks of hydrogen, nitrogen, carbon, and oxygen. Machines capable of printing simple protein structures and other biological materials have already been built by University of Illinois chemist Martin Burke [5], [6] and researchers from Carnegie Mellon have successfully printed a human heart [7]. Consumer advocates and the medical industry have reason to believe that these advances will dramatically lower the costs of highly specialized medications needed to fight aggressive cancers and other disease. The potential social benefits of this technology are obviously immense. If, however, the history of 3D plastic printers is at all illustrative, it seems a forgone conclusion that such advanced 3D printing technology will also be repurposed to produce weapons.

Desktop 3D metal printers and computer-controlled desktop routers for machining metal are already capable of producing high-quality liners for shaped charges and Explosively Formed Penetrators (EFPs). Advanced printers capable of assembling one's medication would likely by design also be capable of producing high-quality explosives like RDX and HMX. Thus, successive generations of wiki weapons will likely be far more capable than their predecessors. Instead of single-shot pistols, curious wiki weapons tinkerers (or terrorists) might be able to produce high quality anti-armor IEDs without the

network of support and specialized equipment production of such devices presently require. Future IED production networks, enabled by advanced 3D printing, will exhibit far less vulnerability to interdiction than their present-day counterparts. For example, bulk purchases of suspicious materials will no longer serve as a “red flag” for those agencies tasked with the interdiction of illegal weapons manufacture, as legitimate use of the required materials would likely be very common.

Another disruptive technology, cryptology, has been the center of controversy since the so-called “Crypto Wars” in the mid-1990s where the U.S. government attempted to classify cryptology as weapon and install “clipper chips” in the personal devices of American citizens [8], [9]. The “clipper chips” themselves were hacked and the issue was promptly dropped on the grounds that the regulations were unenforceable and possibly unconstitutional. The issue has resurfaced again in the wake of the San Bernardino terrorist attack on December 2, 2015, and the FBI’s inability to access the cell phone of Sayed Farooq, one of the attackers. The outcome of the FBI’s attempt to compel Apple to circumvent the security features on Farooq’s phone was inconclusive as an anonymous third party, widely believed to be the Israeli firm Cellebrite [10], was able to hack Farooq’s iPhone after weeks of analysis. Regardless, hundreds of other encrypted communications applications will likely confound future investigations. Further complicating the issue, many of these applications have been developed in jurisdictions not subject to U.S. law.

Former National Security Agency (NSA) contractor Edward Snowden’s revelations indicate several limitations of American and foreign surveillance efforts in the wake of the emergence of easily implementable cryptographic technologies. Browsers like TOR (The Onion Router) and the disk encryption system Truecrypt, when used correctly, have complicated NSA collection efforts [11]. Recent news seems to indicate that the NSA has been able to at least partially penetrate these technologies in the intervening four years. With open-source codes and rapidly rising demand for secure chat applications like Signal however, the state of the art in personal privacy and anonymity is changing every day [11], [12].

Disruptive technologies like cryptology and the blockchain have led to other novel inventions like cryptocurrencies, Bitcoin being just one of a growing number [13–16]. Bitcoin alone has allowed for near total anonymity in commerce, giving rise to alternative marketplaces on the so called “Deep Web” such as The Silk Road. Even after The Silk Road was shut down, numerous other online vendors flourished [13]. When Cyprian officials attempted to confiscate large sums of money from wealthy depositors to cover sovereign debt payments, Euros deposited in Cyprian accounts were anonymously exchanged for Bitcoins almost overnight and then exchanged again into the currency of whatever tax haven had been chosen [14], [15]. Moreover, because Bitcoin maintains a public ledger of all “transactions,” it has proven remarkably secure and is giving some people reason to question the need for state-mandated monopolies like the U.S. Federal Reserve. Additionally, a small but ever-growing amount of economic activity is conducted outside the scope of centralized oversight, further undermining the legitimacy of various regulatory agencies in the eyes of many. Government-sponsored enterprises (GSEs), public institutions and regulators are not the only parties to be threatened by implementations of blockchain technology. Brooklyn-based software developer ConsenSys aims to provide the same services as Google, utilizing a distributed network of computers that synchronizes information exchange via a blockchain implementation known as Ethereum [16].

In the era of technological “black swans,” both society and legacy institutions (be they military or civilian) must learn to rapidly adapt to an individual’s ever-changing capabilities landscape. Before one can properly adapt to these changes, one must first understand their magnitude. We provide a method to assess the impact of such a change and, if possible, determine effective interdiction plans against project networks in which a new, disruptive technology might be in play. To do so, we will utilize decision critical path method (decision CPM) models to analyze the changes in network structure and resiliency that take place when an adversarial network engaged in the production of powerful explosives like RDX for the purpose of constructing anti-armor IEDs, gains access to a disruptive technology like advanced 3D printers.

C. LITERATURE REVIEW

Decision critical path method (CPM) models and other program evaluation and review technique (PERT) models have been used to manage complex industrial tasks such as manufacturing and distribution of drugs and weapons [17]. Interdiction models, such as those in Brown et al. [18], Skroch [19], Brown, et al. [20] and Nesbitt [21] have been used to determine how to optimally delay such a project. We will use such models to illustrate the increased resiliency of future illicit networks that are enhanced with disruptive technologies, such as advanced 3D printers. Those technologies which significantly alter the results of the decision CPM model, should receive the designation of "disruptive" while those which do not significantly alter the results as simply "novel."

D. HOW DO WE DETERMINE WHAT IS DISRUPTIVE?

Disruptive technologies shorten critical paths and/or increase the resiliency of a network. We thus introduce a model for the building of sophisticated anti-armor IEDs, utilizing present-day technology. We also introduce a model for the building of such weapons using a disruptive technology like advanced 3D printers, capable of printing explosives from simple feedstocks of common elements like hydrogen, nitrogen, oxygen, carbon and possibly utilizing cryptographic technologies to anonymize acquisition of CAD files for explosive materials. Attacker extensions are implemented in both models in an effort to stop or delay the production of these weapons.

Networks have been used singularly to model decision CPMs [22]. When represented as such, the time to complete the project is the length of the longest path through the network, also referred to as the critical path. The operator seeks to minimize the length of this path as much as possible. The attacker seeks to maximize it. By comparing changes in the length of the critical paths of both models we will be able to make the determination as to whether a technology is truly disruptive. Only those technologies that significantly shorten the length of the critical path despite the best efforts of someone trying to interdict the project should be classified as disruptive.

E. HOW TO HANDLE FUTURE DISRUPTIVE TECHNOLOGIES

Few, if any, quantitative analysis tools presently exist to inform decision makers about the impacts of any given disruptive technology. Leadership must make do with the advice of purported experts claiming to have the ability to foresee the "unknown unknowns" or "black swans" on the horizon. Whatever merit this method may have, it is difficult for objective science to quantify. In an effort to remedy this, it is the purpose of this thesis to advance the use of flexible and adaptive modeling tools that can be rapidly implemented once a disruptive technology emerges. Decision CPMs can be developed and analyzed to determine the impacts of future disruptive technologies when these can be represented as partially ordered tasks in a project in relatively little time. What is more, decision CPMs can provide realistic estimates of one's ability to interdict or delay those actors employing a disruptive technology. These qualities make decision CPMs the ideal choice for aiding leadership in making intelligent decisions regarding emergent disruptive threats.

II. MODELING THE EFFECTS OF DISRUPTIVE TECHNOLOGY

A. DECISION CPM

The disruptive technology, or DISTECH, model considers a series of interdictions across two separate project management models to determine an optimal attack set against an adversary project network. An optimal attack is the one which maximally lengthens the operator's critical path (i.e., maximally delays project completion time). It considers production projects utilizing both present day and projected future disruptive technologies to quantify anticipated changes in network resiliency and structure. We use standard project management software (e.g., Microsoft Project [23]) to represent the tasks required for completion of the operator's project, as well as precedence relationships among project activities, and the decisions regarding procurement methods. The objective of the operator is to choose the optimal path to complete his project despite the interdiction efforts of the attacker. The attacker seeks to optimally delay, and if possible stop, the industrial project of the operator. Disruptive technologies are considered to be those technologies that either significantly shorten the operator's chosen critical path or significantly degrade the attacker's ability to interdict that path though the network.

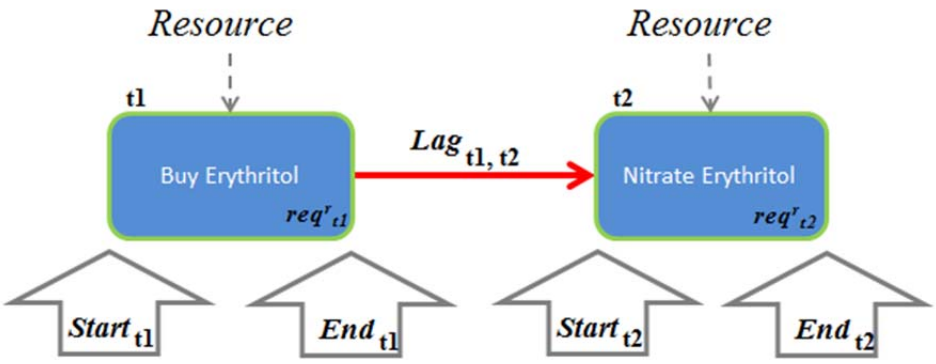
B. PROJECT NETWORKS

Project networks have been used extensively to model these types of processes [21], [22]. Moder, Phillips, and Davis specifically define a *project* as a distinct family of *tasks*. Each task has a specified *duration* and may require a finite amount of *resources* to complete. Additionally, these tasks have specified *precedence* relationships between their ordered pairs. Some tasks may also have a specified amount of *lag* in between the *completion time* of the first task, referred to as the *predecessor* in the ordered pair, and the earliest possible *start* time of the subsequent task called the *successor* in any given ordered pair [21],[22].

Network diagrams are used to represent these tasks and associated precedence relationships. Tasks are represented as nodes. In this network diagram (see Figure 1),

nodes are drawn as rectangles with rounded corners. An arc, usually drawn as an arrow from the rightmost edge of predecessor task to the leftmost edge of the successor task, represents the precedence relationship between the two tasks [21], [22]. One such precedence relationship between tasks t1 (Buy Erythritol) and t2 (Nitrate Erythritol) is illustrated in Figure 1. Project management tools take these network models (including their tasks, precedence relationships, task durations, resource availability etc.) as inputs and produce an optimized schedule for completion of the tasks in the project. A schedule is considered feasible if it has start and end times that honor task durations, lag times, precedence relationships and resource constraints. A schedule is deemed optimal if it is both feasible and provides the earliest possible time for project completion [21], [22].

Figure 1. Illustration of Precedence Relationships



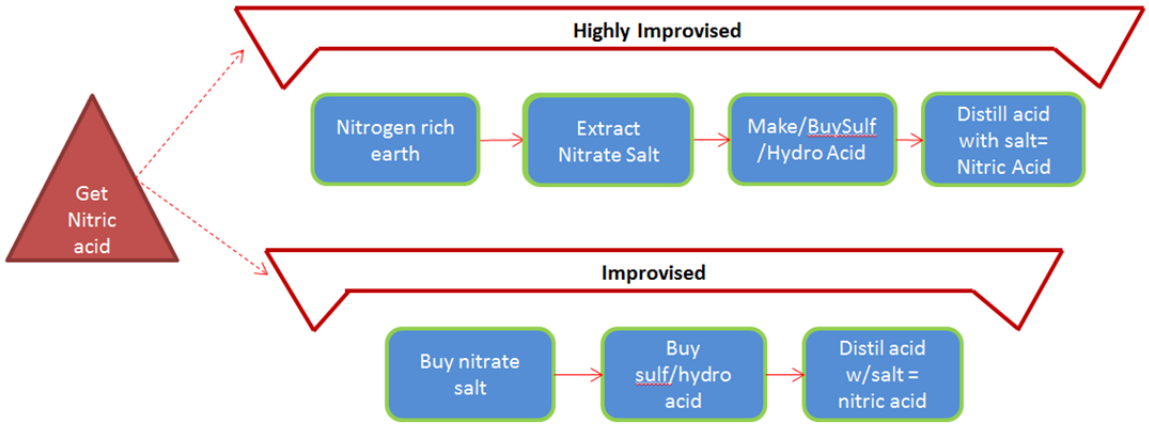
Two tasks, t1 (Buy Erthritol) and t2 (Nitrate Erythritol) are shown with the proper precedence relationship. The time required to complete t1 is the difference between t1's START and END time. A specified lag time ($Lag_{t1,t2}$) must elapse before task t2 can start. It is possible for $Lag_{t1,t2}$ to be equal to zero. The horizontal arrow represents the precedence relationship between t1 and t2. The grey dotted arrows above the tasks represent the flow of the necessary resources into the task nodes. The types and quantities of resources needed to complete a task is represented by req^r_{t1} and req^r_{t2}.

In project network models, strict task dependence must be enforced from the start task to the finish task. This task dependence is illustrated above via the arrow from t1 (Buy Erythritol) to t2 (Nitrate Erythritol). As a task ends, a lag time measured in days is initiated. It is possible for this lag time to equal zero or less. Upon completion of this lag

time, the next task (the successor) can begin. In a majority of cases, all predecessors must be complete before a successor task can begin.

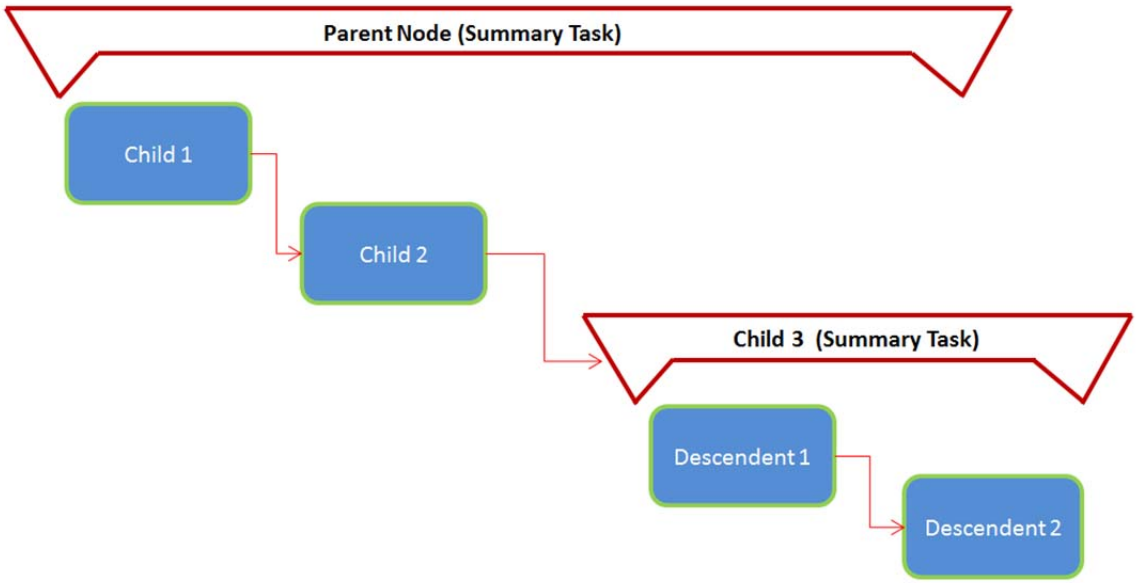
Decision nodes represent tasks that only require one (or some) successor tasks to be completed. Decision nodes allow us to model alternative means of preparing for a task. One of the best examples of this is demonstrated in Skroch [19] whereby the author provides three alternative means for the enrichment of weapons grade uranium [19], [21]. Figure 2 is an example whereby the operator is able to pursue two separate means of acquiring an important precursor chemical, nitric acid. In the DISTECH model, the operator chooses which method he wishes to use to procure nitric acid, Highly Improvised or Improvised. Both the Highly Improvised and Improvised nodes are referred to as Summary Tasks. The tasks that constitute the Highly Improvised and Improvised methods of producing nitric acid are called child nodes. It is possible that some of these child nodes are summary tasks themselves. The tasks that make up these child summary tasks are referred to as descendent nodes. This relationship structure is depicted in Figure 3.

Figure 2. Decision Node Example



The decision node (task) "Get Nitric Acid," only requires one of the two parallel sets of subordinate summary tasks to be completed for the operator to acquire nitric acid, a precursor chemical used for the manufacture of the explosives RDX, a secondary explosive, and ETN, a booster explosive.

Figure 3. Parent, Child, Descendent Node Relationships



C. ASSUMPTIONS

The following assumptions are made throughout the DISTECH model.

- The operator behaves optimally in order to complete the project
- The operator always pursues those tasks that will result in the quickest completion of the overall project.

- Operator is aware of the interdiction efforts of the attacker and allocates his efforts accordingly
- The attacker will always attack the vulnerable nodes that lengthen the critical path the most.

D. FORMULATION

The DISTECH operator model is an integer linear program. That operator model is implemented as a decision-CPM. The attacker extension influences the duration of the operator CPM. The operator model seeks to find the shortest critical path through the project network, thus resulting in the earliest completion time possible. DISTECH allows the operator to choose various options for completing his project via binary decision variables that serve to track the operator's progress. The attacker model imposes penalties on vulnerable tasks to optimally delay the operator. These penalties often force the operator to choose processes that, while they may be invulnerable to attack, result in significant delays in the project's completion time.

1. The Operator Model

SETS

$k \in K$	Tasks (nodes**)**
$(i, j) \in P \subseteq K \times K$	Precedence Relationship. Task i precedes task j (arcs)
$s \in S \subset K$	Summary Tasks
$d \in D \subset S$	Decision Summary Tasks
$k \in K_s \subseteq K$	Children of Summary Task *k*
$start \in K$	Distinguished Start Task
$finish \in K$	Distinguished Finish Task

PARAMETERS

d_k	Duration of task *k* [days]
$lag_{i,j}$	Required delay between completion of task *i* and start of *j* [days]

VARIABLES [units]

Z	Objective [days]
EST_k	Earliest start time for task *k* [days from start]
$COMPLETE_k$	Task *k* completed [binary]

FORMULATION

$$\begin{aligned}
\min \quad & Z = EST_{finish} && && (a0)\\
s.t. \quad & EST_j - EST_i \geq (d_i + lag_{i,j}) * COMPLETE_j && \forall (i,j) \in P && (a1)\\
& \sum_{k \in K_d} COMPLETE_k \geq COMPLETE_d && \forall d \in D && (a2)\\
& COMPLETE_k \geq COMPLETE_s && \forall s \in S \setminus D, k \in K_s && (a3)\\
& COMPLETE_{start} \equiv 1 && && (a4)\\
& EST_k \geq 0 && \forall k &&\\
& COMPLETE_k \in \{0,1\} && \forall k &&
\end{aligned}$$

DISCUSSION

Each project has a final set of tasks completed in set *K*. A project is complete when a set of tasks in *K* connects tasks designated as *start* and *finish* in the set *K*. The objective function (a0) expresses the estimated time to completion of the project, measured in days. Each constraint (a1) ensures that the earliest start time for a task is greater than or equal to the completion time of each of its predecessors, plus any lag time between the two tasks [21], [22]. Each constraint (a2) requires that at least one child of a completed decision node is also completed. Note that each decision node is a summary node, and so the notation K_d is consistent with our definition of K_s. Each constraint (a3) ensures that if a non-decision summary task is completed, each of its children is completed. Constraint (a4) ensures the *start* task is completed, thus ensuring the entire project is completed with a feasible set of decision nodes and their resulting subtasks completed.

2. The Attacker Model

The attacker model seeks to maximally delay the completion time of the operator model by lengthening its critical path. The attacker model also operates on both operator project models. In the attacker model, attack sets can change based on the assumed vulnerability of a given node to interdiction.

In the base case, all nodes (tasks) in both operator project models are considered vulnerable to interdiction. This results in the attacker model rapidly imparting significant

delays on the operator, possibly extending the earliest start date of the *finish* task to a virtual infinity. This effectively stops the operator entirely. Assuming that all nodes in the operator model are vulnerable may not reflect reality. Many tasks in the project model constructed to motivate the discussion concerning the DISTECH model (the production of IEDs), require only the most rudimentary resources [24].Therefore, assuming all nodes in the network are vulnerable to interdiction leads to excessively optimistic estimates about the attacker's capability to delay the operator. Thus, in an effort to make the results of the attacker model more realistic, we make certain nodes (tasks) invulnerable to attack. The attacker model is agnostic about the actual means of attacking vulnerable nodes. The attacks can come in the form or kinetic operations or otherwise. The only pertinent information required is that a plausible means of interdiction exists and an estimate of the amount of delay imparted on the operator model should such an interdiction take place. After our baseline "total vulnerability" assessment, we then begin to consider only plausible attacks.

DISTECH Attacker Model Formulation

DATA [units]

$max\_attacks$	Maximum number of attacks [cardinality]
$delay_k$	Additional delay if task k attacked [days]
pen_skip_k	Penalty for each day of delay skipped on an attacked arc. [Days/day] (Usually 1 unless arc k invulnerable)

VARIABLES [units]

Y_k	1 if task k attacked, 0 otherwise [binary]
$SKIP_k$	Amount of delay on task k to skip [days]

FORMULATION

$$\max \min Z = EST_{finish} + \sum_k .01 * COMPLETE_k + \sum_k pen\_skip_k SKIP_k Y_k \qquad (b0)$$

$$s.t. \quad EST_j - EST_i + SKIP_i \geq (d_i + lag_{i,j} + delay_i) * COMPLETE_j \qquad \forall (i,j) \in P \qquad (b1)$$

$$\sum_{k \in K_s} COMPLETE_k \geq COMPLETE_d \qquad \forall d \in D \qquad (a2)$$

$$COMPLETE_k \geq COMPLETE_s \qquad \forall s \in S \setminus D, k \in K_s \qquad (a3)$$

$$COMPLETE_{start} \equiv 1 \qquad (a4)$$

$$\sum_k Y_k \leq max\_attacks \qquad (b2)$$

$$0 \leq SKIP_k \leq delay_k \qquad \forall k \in K \qquad (b3)$$

$$EST_k \geq 0 \qquad \forall k \in K$$

$$COMPLETE_k \in \{0,1\} \qquad \forall k \in K$$

$$Y_k \in \{0,1\} \qquad \forall k \in K$$

DISCUSSION

Equation (b0), the objective function, expresses the length of the longest path the operator must take through the network, including penalties for skipping any delays that attacks might impose. Similar to constraint (a1), constraint (b1) ensures that the earliest start time for the next task is greater than or equal to the completion time of its predecessor plus any delay; if the task has not been attacked the operator can skip this delay at no cost. Constraints (a2), (a3) and (a4) are identical to the constraints in the basic operator model and constrain the operator's actions in the same ways. Constraint (b2) sets an upper bound on the number of attacks that can be carried out against a project network. Constraint (b3) establishes an upper bound on the duration of the delay that can be skipped for a given task, assuming the task has not been attacked. If this constraint were not enforced, it would become possible for the operator to shorten the task's original, non-interdicted duration.

3. Solving the Attacker Problem with Decomposition

Given a fixed set of attack values, $\hat{Y}_k$, the resulting operator problem has a modified objective function:

$$\min Z = EST_{finish} + \sum_k .01 * COMPLETE_k + \sum_k pen\_skip_k SKIP_k \hat{Y}_k \qquad (c0)$$

If we solve the operator decision CPM model with this modified objective function for a particular attack, we will find the operator's *optimal response* to that attack. This parameterized operator's model (using (c0) as the objective and (a1)-(a4) as the constraints) becomes the *subproblem* in a decomposition algorithm for solving the attacker's problem. For any particular operational plan, given by values $\overline{EST}_k$, $\overline{COMPLETE}_k$, and $\overline{SKIP}_k$, the expression

$$\overline{EST}_{finish} + \sum_k .01 * \overline{COMPLETE}_k + \sum_k pen\_skip_k \overline{SKIP}_k Y_k \qquad (d0)$$

calculates the processing time with delay (in days) an attacker can inflict on that particular operational plan, and therefore provides an upper bound on the amount of delay that can be inflicted in the worst-case scenario for any possible response the operator might have. The corresponding *master problem* at any particular iteration, *ITER*, collects all of the operator plans seen so far (indexed by iteration number, *iter*) and creates a bound on the optimal attack for each one.

PARAMETERS

$\overline{EST}_{k,iter}$	Start time of each task in plan *iter*
$\overline{COMPLETE}_{k,iter}$	Indicates whether task *k* completed in plan *iter*
$\overline{SKIP}_{k,iter}$	How much of the delay on task *k* was skipped in plan *iter*

VARIABLES [units]

Z_MP	Master decomposition problem objective surrogate [days]

MASTER PROBLEM FORMULATION

$$\max_{Y} \quad Z_{MP} \qquad (\text{m0})$$

$$Z_{MP} \le EST_{finish,iter} + \sum_{k} .01 * COMPLETE_{k,iter} + \sum_{k} pen\_skip_{k} SKIP_{k,iter} Y_{k} \quad \forall iter \le ITER \qquad (\text{m1})$$

$$\sum_{k} Y_{k} \le max\_attacks \qquad (\text{b2})$$

$$Y_{k} \in \{0,1\} \quad \forall k$$

DISCUSSION

The objective (m0) represents the most damage an attacker can do to the project network. Each constraint (m1) is called a "cut" and provides an upper bound on that maximum damage based on a particular operational plan. See Alderson et al. [25] for a detailed discussion of decomposition formulations and algorithms for solving Attacker-Defender models.

For the first iteration of the decomposition no tasks are attacked, and the resulting subproblem finds the fastest way to complete the non-interdicted project. That plan is the added to the master, which is solved to determine the worst attack against it. Every time a subproblem is solved the resulting objective value provides a lower bound on the damage an attacker can do (because it determines the operator's best response to a particular attack), and that operational plan is added as a new cut to the master (m1).

Every time the master problem is solved it has one more constraint than in the previous iteration, and therefore the sequence of optimal objective values are non-increasing, and each provides an upper bound on the optimal attack value.

At each iteration we retain the best lower bound seen so far (and the corresponding *incumbent* attack), and we terminate if the difference between the upper bound and the best lower bound is within a tolerable number of days.

Each time the sub-problem is solved, it produces one of these "cuts" which is then added to the master problem. If repeated operational plans are detected we add a set of solution elimination constraints to ensure a different path for project completion is

evaluated. We cannot use the resulting operational plans to create a lower bound on such an iteration, but that plan will add a valid cut to the master problem, ensuring the eventual convergence of the algorithm [25].

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESULTS AND ANALYSIS

The results of the DISTECH model, operating on both the Legacy and Advanced project networks, are summarized in Table 1.

Table 1. Table of Results

Project Model	Project Duration (Days)	Delay (Days)
Legacy Project (Invulnerable)	32.5	0
Legacy Project (Completely Vulnerable)	∞	∞
Legacy Project (Feasible Interdiction I)	39.5	7
Legacy Project (Feasible Interdiction II)	45	12.5
Advanced Project (Invulnerable)	15	0
Advanced Project (Completely Vulnerable)	∞	∞
Advanced Project (Feasible Interdiction)	20	5

The DISTECH decision CPM model determines the optimal operator plan. The analyst is generally regarded as an attacker. Once the optimal operator path is chosen, the attacker extension implements an interdiction regime designed to inflict maximal delay on the operator. By comparing the ability of the attacker to lengthen the critical path of the operator model in both project models, an analyst can begin to make determinations as to whether a candidate technology is disruptive. The application of this model on two notional IED producing networks demonstrates how this process works.

A. THE NON-INTERDICTED LEGACY PROJECT

In order to illustrate the effects a disruptive technology will have on an adversary's project network, one must first model a base case with no interdictions. First, we will examine what a project model might look like for a network engaged in the construction of anti-armor IEDs utilizing present-day technology, henceforth referred to as the legacy project. Specifically, this network is involved in acquiring explosives with high brisance like RDX (nitrated hexamine) that are suitable for forming high velocity

projectiles and plasma jets from a ductile metallic liner which is in turn capable of piecing heavy armor.

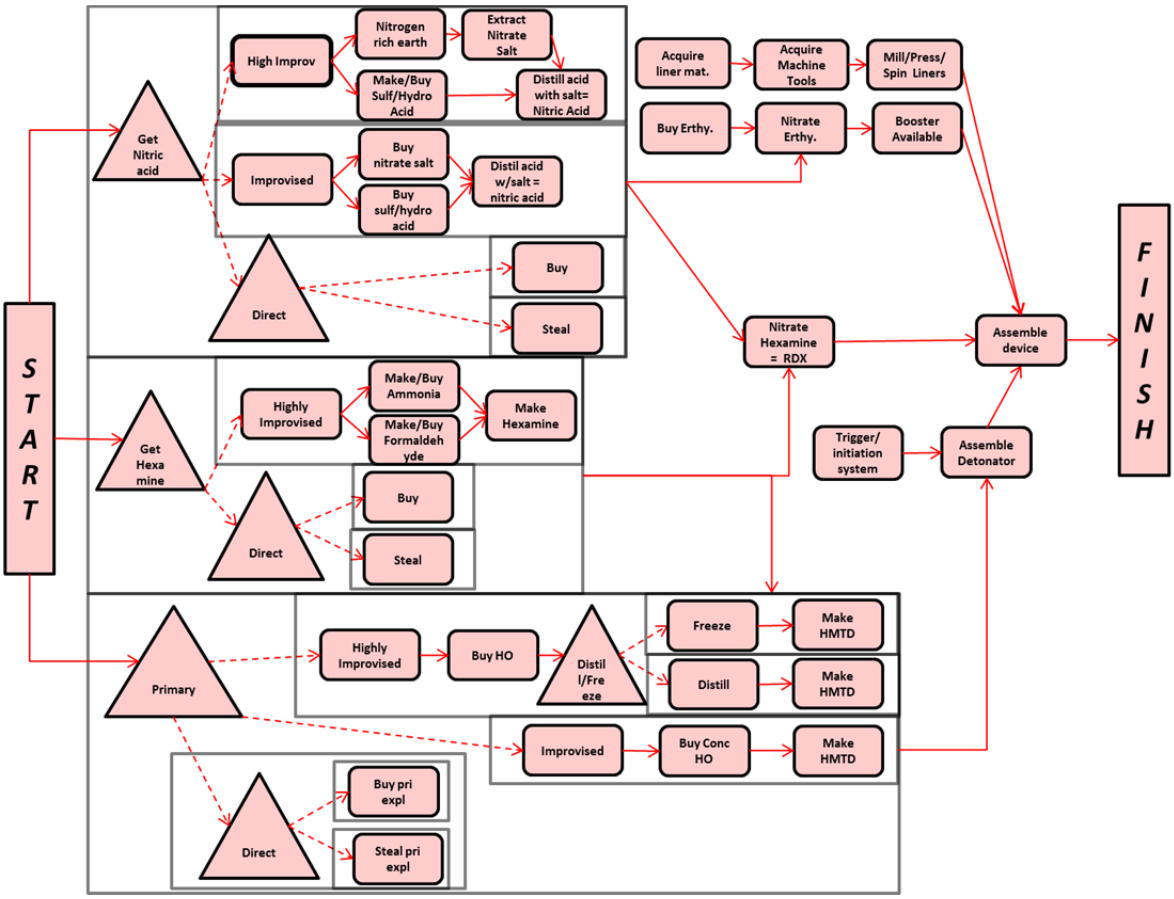
Additionally, the legacy project must acquire primary explosives to initiate the explosive train and a booster explosive to ensure sufficient shock has been imparted to the secondary explosive (a.k.a. main charge). Access to commercial or military blasting caps can greatly aid any would-be bomb maker as they tend to be safer and more reliable. Access to such materials is closely regulated in the West as few legitimate uses exist outside of commercial demolition, mining and certain agricultural applications. Therefore, one must consider some of the common improvised methods of acquiring primary explosives for use in improvised blasting caps. In this case, we will consider common methods for acquiring a peroxide based home-made explosive, HMTD. HMTD is somewhat less sensitive to shock and friction than its peroxide based cousin TATP which was used in the 2005 London bombing which killed 56 and injured over 700 [26]–[28]. Both explosives are easily improvised from common chemicals that have numerous legitimate uses; however, both explosives require considerable care in their manufacturing and handling [24], [27], [28]. Common household items that can be used in explosives manufacture are depicted in Figure 4.

Figure 4. Possible Precursors for Explosives Manufacture

Common household items that can be used as feedstocks for clandestine explosives manufacture are depicted above. An exhaustive list is virtually impossible to assemble. While the collection of large quantities of these precursors may be indicative of illicit activity, effective monitoring of purchases of such common items is exceedingly difficult and other indicators are likely needed.

In order to complete the legacy project, the network must acquire the tools (lathe, hydraulic press, etc.) to produce the liners as well as an initiation mechanism. The potential combination of common materials that can be turned into an effective initiator are too numerous to count. Any conductive piece of metal can be used to close a simple electric firing circuit while common household items like exterior lighting motion sensors and cell phones have been used to initiate IEDs. Since the possibilities are so numerous, the tasks associated with the construction of such IED components are summarized into only a few generic tasks. Combining all these components completes the project. This task is visually depicted in the network as the “Assemble Device” node in Figure 5.

Figure 5. The Invulnerable Project Network



The non-interdicted Legacy model completes in 32.5 days, assuming the task durations provided in the model are reasonably accurate. This represents the "best case" scenario for an operator whom is assumed to be attempting to remain "undetected" throughout the acquisition of their required precursor materials. Dashed lines indicate choices on the part of the operator. Solid lines indicate tasks that must be completed after the operator has made a decision about which method to use in procuring a given bomb component.

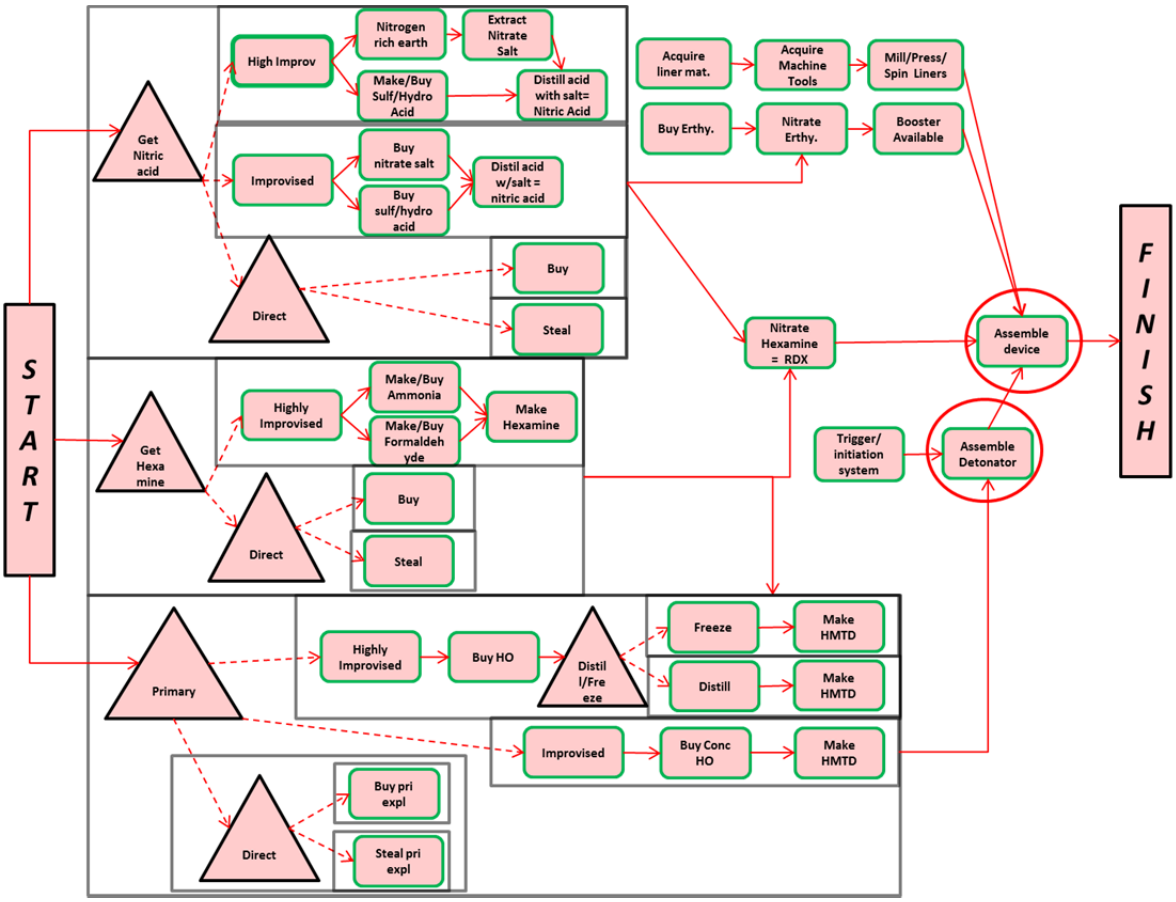
B. THE COMPLETELY VULNERABLE LEGACY PROJECT

We next introduce a version of the Legacy project model where all tasks are vulnerable to interdiction. The attacker extension of the DISTECH model seeks to interdict those tasks which will maximally delay the project completion date. This particular attack set assumes the attacker has both a perfect knowledge of the operator's network structure and a credible means of interdicting any given task.

In the case of total vulnerability, the DISTECH attacker extension favors interdictions towards the end of the project, as illustrated in Figure 6. This is because

tasks in later stages of the project must be completed because there are no alternatives. This does not mean that no alternatives exist. Additionally, it is assumed that interdictions at this point in the project essentially destroy the IED network by capturing the bomb makers, their equipment and stores of precursor chemicals and ready-made explosives. This is reflected in DISTECH by making the delay associated with the interdiction of those tasks immense, thus stretching the length of the critical path to a virtual infinity.

Figure 6. The Completely Vulnerable Project Network



Green borders represent vulnerable tasks in the project network. Large red circles indicate tasks interdicted by the DISTECH attacker extension. Attack budget has been set at two interdictions.

C. FEASIBLE INTERDICTION REGIMES OF THE LEGACY PROJECT

Interdicting the most critical tasks in a network may not always be possible. This is especially true if the network operator is utilizing tools and materials that have numerous legitimate uses. Moreover, the attacker may lack the level of knowledge of the operator's network structure and intentions required to carry out the type of attack in the previous interdiction regime. This is especially true in the era of self-radicalizing terrorism.

One must thus consider how to impose delays on the operator model earlier in the project without highly detailed knowledge of its structure or the intentions of the operator. Such interdictions often take the form of regulations and licensing requirements or overt surveillance to discourage or prevent the operators of illicit networks from acquiring the tools necessary for advancing their agendas too easily. In the case of the legacy project network, such interdictions take the form of the ATF's Limited User permitting for the purpose of screening individuals before purchasing blasting caps and other explosive materials [1]. Additionally, surveillance of known distributors of bulk amounts of common precursor substances like nitric acid or ammonium nitrate is considered to be plausibly implementable. Both actions impose significant delays on the operator as he must now pursue more clandestine methods of sourcing the required materials to make IEDs in any significant quantity.

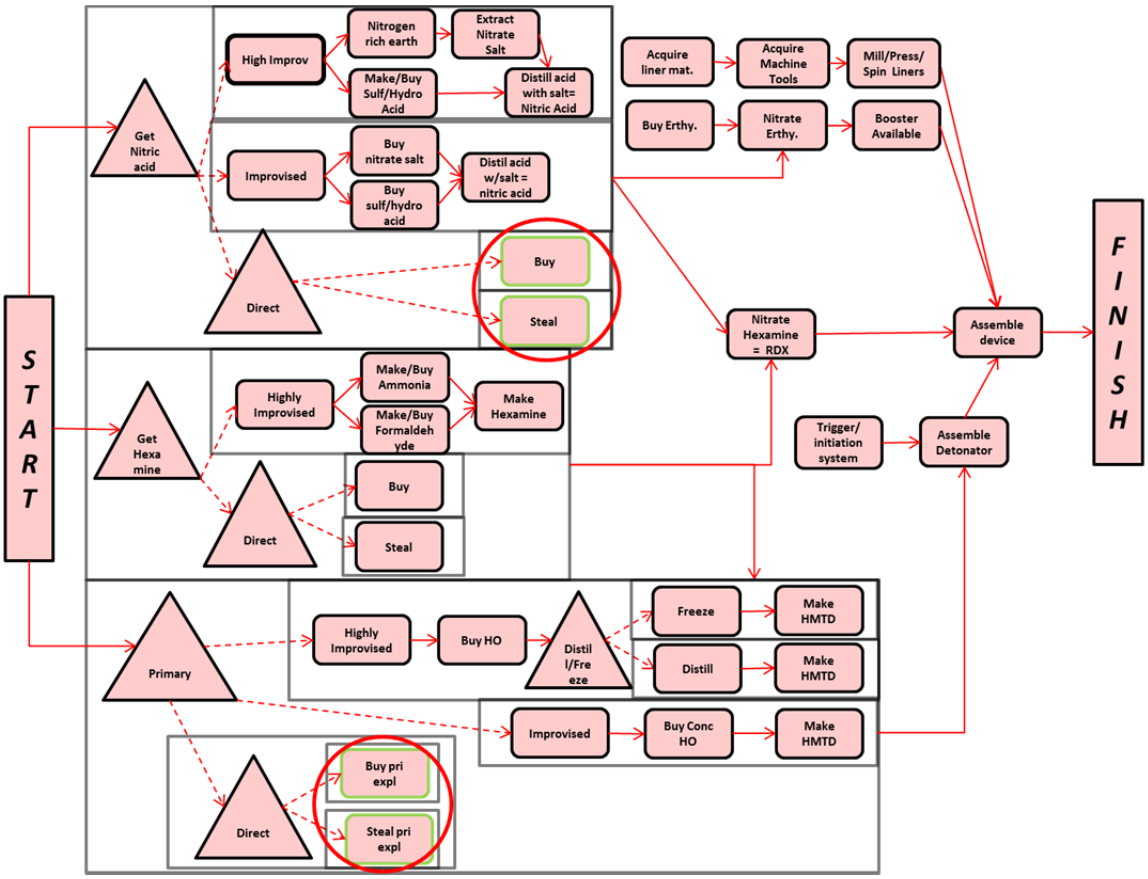
Restricting access to primary explosives via both licensing and physical security requirements lengthens the critical path by approximately 23% (40 days vice 32.5) as alternative procurement methods exist. Additionally, the operator is forced to procure nitric acid by first procuring other common acids like sulfuric acid (drain opener, car batteries) or hydrochloric acid (a.k.a. muriatic acid, used to clean pools) and distilling it with a nitrate salt like ammonium nitrate, potassium nitrate, or sodium nitrate (e.g., instant cold packs, tree stump remover, saltpeter, curing salt). The operator is also forced to improvise primary explosives as his access to commercial and military grade blasting caps is now restricted. While the production of the primary explosives used in improvised blasting caps is relatively easy, it can be very dangerous to those not familiar with the process as the peroxide based primary explosives considered in this network are quite

sensitive to shock, friction and heat [27],[28]. Alternatives exist in the form of mercury fulminate and lead azide; however, their synthesis is not considered [24], [28]. All of these processes require the operator to expend considerable amounts of time to both acquire precursors and then manufacture the explosives.

Some tasks are considered invulnerable to interdiction, such as those tasks associated with the "highly improvised" method of acquiring nitric acid. This method involves harvesting nitrate salts from nitrogen rich earth, a process recorded by Roger Bacon in 1267 [27]. Any nitrogen-rich soil (i.e., compost, dung, and soil mixtures from stables) can be used to extract potassium nitrate [24]. Clearly, no plausible means exists to prevent persons from gaining access to dirt, wood ashes, a bucket, and the other rudimentary supplies required to extract nitrate salts. Thus, tasks associated with such processes are considered invulnerable. While such processes are immune to the attacker's interdiction efforts, they do require a significant amount of time to extract a useful amount of nitrate salts (see Figure 7) [24]. If the attacker can successfully force the operator to pursue such primitive methods, the attacker is doing very well indeed.

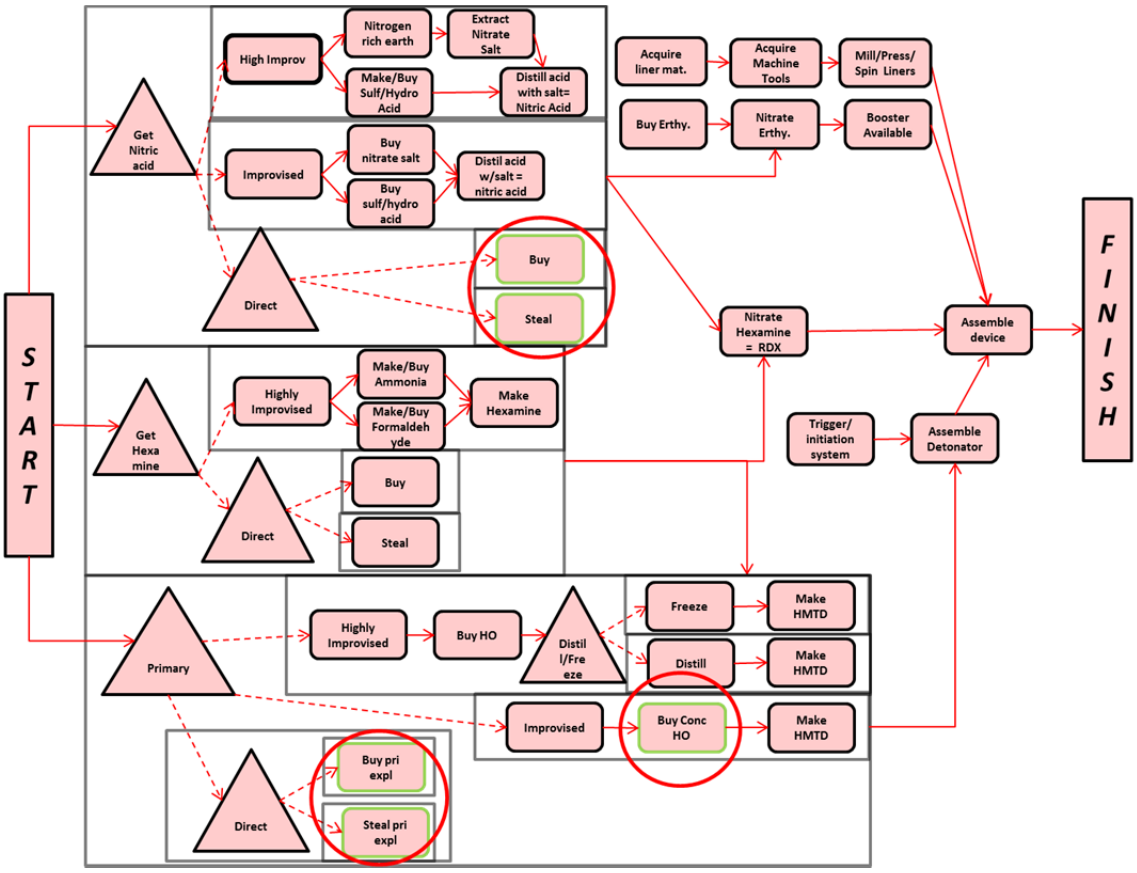
Other tasks remain vulnerable in the legacy project network as well. For example, the bulk purchase of concentrated hydrogen peroxide (~20–30%) may serve as an indicator of illicit activity although not as clearly as nitric acid or explosives from licensed retailers. Concentrated hydrogen peroxide (CHP) solutions have various legitimate uses ranging from hydro and/or aquaponics to papermaking and many more. While likely to be time consuming, the monitoring of bulk CHP solutions and its vendors might be possible. Obviously, this burden can be considerably lightened if the attacker has other indicators of illicit activity or specific intelligence about the intentions of the network operator. When combined with the previous interdictions, the interdiction of easy access to CHP lengthens the critical path to 45 days and is depicted in Figure 8.

Figure 7. Primary Explosives and Nitric Acid Interdiction



By simply restricting access to primary explosives (i.e., blasting caps) and monitoring large purchases of nitric acid, the critical path can be lengthened by approximately 23%. Attack budget has been increased to four interdictions.

Figure 8. Primary Explosives, Nitric Acid, and CHP Interdiction

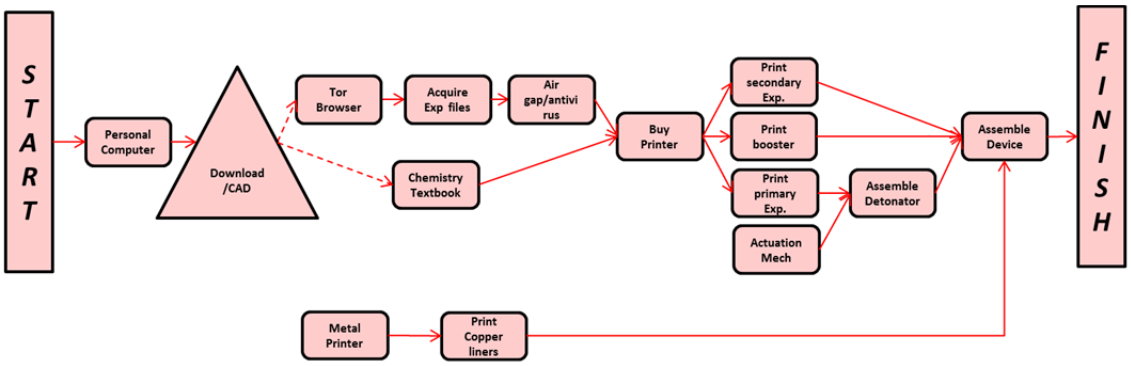


By limiting access to primary explosives and monitoring bulk nitric acid and CHP purchases, the critical path can be extended to 45 days, a 38% increase from the non-interdicted network. Attack budget has been set at five interdictions.

D. THE NON-INTERDICTED ADVANCED PROJECT

We will now model a clandestine IED network that utilizes an advanced 3D printer capable of manufacturing molecules out of simple feedstocks of basic elements. By assessing the changes that take place in the network's structure and task durations when a new technology is introduced we will be able to gain insight into whether a particular technology is disruptive or not. The non-interdicted advanced project network is able to complete its task much more quickly than the legacy project. In this case, it would require the network operator only 15 days to complete his project.

Figure 9. The Non-Interdicted Advanced Project Network

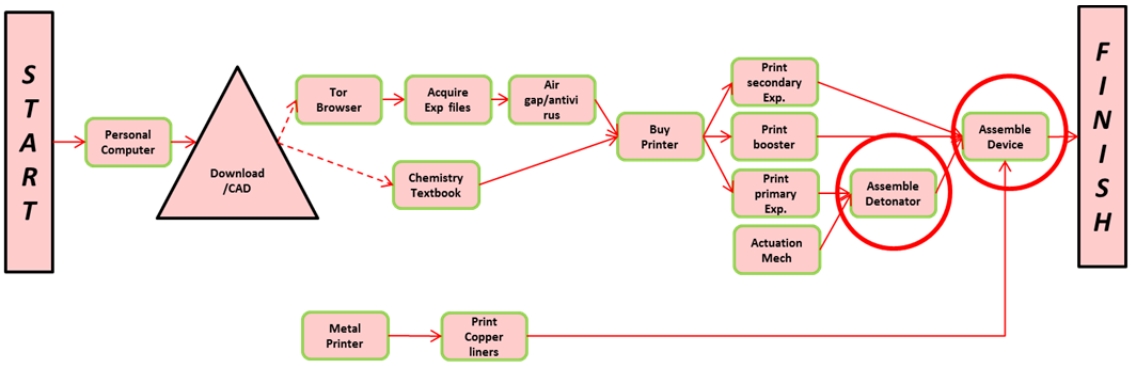


The non-interdicted advanced project network which utilizes advanced 3D printing technology. This project completes in as little as 15 days.

E. TOTALLY VULNERABLE ADVANCED PROJECT

The advanced project network is initially assessed as though it were totally vulnerable. Like the legacy project network, the DISTECH attacker extension favors "necking" tasks that all potential paths must pass through. In this case, if the attacker can again interdict the operators during final device assembly, the attacker effectively kills the advanced project network. It is plausible that an attacker might receive intelligence from some other source and interdict the operator during final device assembly. Again it is assumed that interdiction during this task effectively stretches the length of the critical path into infinity. If it could be assumed that an attacker could consistently interdict such a network during this phase of the project, an advanced 3D printer-enabled IED network would not be considered a disruptive technology.

Figure 10. Totally Vulnerable Advanced Project Network



If an attacker is able to interdict either of the tasks circled in red, the critical path effectively lengthens to infinity. If it were plausible to consistently interdict such a network during these stages of the project, advanced 3D printing technology would not be considered disruptive.

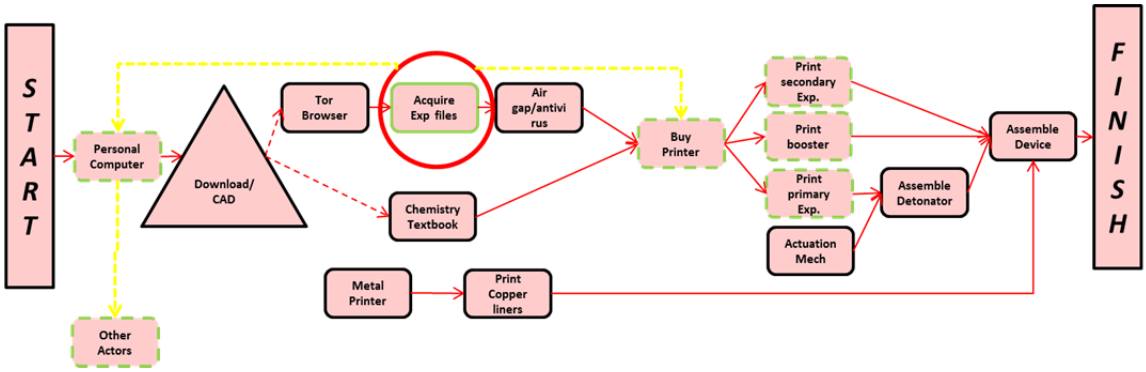
F. FEASIBLE INTERDICTION REGIMES OF THE ADVANCED PROJECT

It is unlikely an attacker would consistently possess the level of knowledge required to continually interdict the advanced project model at the points specified above. To that end, more plausible interdiction efforts appeal. Experts currently debate whether the regulation of the advanced chemical "inks" required by such machines would be effective in the long term [29]. Additionally, it would seem intuitive that operators would want printers capable of working with a wide range of basic elements for maximum utility. Since compounds found in explosives typically consist of chemical bonds of elements like hydrogen, nitrogen, carbon, and oxygen, which all have an innumerable amount of legitimate uses in day-to-day life, clandestine activity would likely hide in plain sight. Thus, another method for attacking or delaying the operator must be considered.

It is widely believed the Stuxnet computer virus was developed during the Bush administration to sabotage the Iranian nuclear weapons project. Sometime in 2010, the Obama administration is thought to have authorized its deployment against the Natanz nuclear facility in Iran as a means of delaying the Iranians from enriching enough weapons grade uranium to develop a nuclear weapon [30], [31]. Similar attacks might be possible against networks employing advanced 3D printers. Since the operator must either acquire the advanced CAD files required to make explosives or design them

himself, the attacker might consider installing malicious code analogous to Stuxnet into CAD files for explosives and posting them online. Such malicious code might also contain advanced spyware to help the attacker better determine the network structure of the project model or to help reveal those who might be collaborating with the operator. If the operator then attempts to utilize the CAD files he has acquired online, a Stuxnet-like virus might activate and render the printer useless.

Figure 11. "Stuxnet" Interdiction and Spyware Insertion



The attacker inserts a computer virus analogous to Stuxnet into the CAD files for explosives and distributes them liberally online in known online extremist forums and file-sharing websites. This attack "enters" the project network via the downloading of the files and interdicts the project at the 3D printer itself. Spyware may also be inserted into the file to help the attacker find other nefarious actors.

The magnitude of such a delay is hard to quantify. The virus effectively renders the printer useless and breaks the network. The delay inflicted on the operator is thus equal to the amount of time it takes him to acquire a new printer. This may prove difficult as the operator may have tipped off the attacker about his activities by downloading and executing the infected files. In such a case, the critical path once again is lengthened to infinity and the network is effectively destroyed.

A plausible alternative for the operator will depend on the sophistication of advanced CAD software that supports the printing of complex molecules. If the sophistication of the software matches that of the printer, it may very well be plausible that the operator could "build" the explosives himself from common text books and references. Doing so would allow the operator to keep the most critical piece of network

infrastructure, the advanced 3D printer, offline and unconnected and thus limit its vulnerability to any form of cyberattack. This results in the overall completion being delayed from 15 days to 20 days.

G. FINAL DETERMINATION

To make the final determination as to whether a technology is truly disruptive, an analyst must now consider the amount of delay the attacker can plausibly impart on the two separate networks. In this case, the legacy network can be delayed an additional 12.5 days until all tasks are completed resulting in a total completion time of 45 days vice 32.5. The advanced project model utilizing advanced 3D printing technologies to manufacture explosives can only have its critical path lengthened from 15 to 20 days. Thus, since the advanced project network completes all required tasks even after the attacker's interdiction efforts far faster than the legacy network under any circumstance, advanced 3D printing technology would earn the designation of "disruptive."

This may not always be the case, however. As both the network operator and the network attacker constantly develop new capabilities, any given technology or process that was once considered disruptive may lose that designation. This implies that new assessments will be required as new capabilities emerge.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSIONS AND RECOMMENDATIONS

There is much more to be hoped for in an excess of information or of weapons than in the restriction of information or arms control.

—Jean Baudrillard

Disruptive technologies shorten critical paths and/or make them more resistant to interdiction. Any network that utilizes a technology that fits this definition is inherently more difficult to delay, degrade, or destroy. The DISTECH model allows an interested party to quantify the magnitude of the resultant changes in project network structure and resilience. In doing so, it offers insight on how one might respond to, or cope with said disruptions. The rapidly implementable, quantitative analysis provided by this process can also suggest ways to organize and manage new intelligence and capabilities requirements to combat nefarious actors who employ them while side-stepping some of the pitfalls associated with trying to predict the future.

To illustrate the effects such a technology might have, we have introduced a project management model of two networks that represent the production of IEDs, one utilizing present-day technology and the other, advanced 3D printers to manufacture key components. We demonstrate how the present-day network may be significantly degraded by attacking tasks and how inflicting similar delays on the network employing advanced technologies is very difficult. In this particular case, we were able to lengthen the critical path of the legacy project by 12.5 days for a total duration of 45 days. We were only able to delay the advanced project model 5 days for a total duration of 20 days. Whether considering the relative magnitude of delay or the absolute value of the time until total project completion, the advanced network's use of 3D printers is clearly disruptive.

Not every new technology is disruptive. Previously, we mentioned the disruptive effects of the printing press. Had the ballpoint pen been invented in the middle of the 15th century instead of the printing press, it is possible the social upheavals of the time might not have reached the same magnitude, as skilled scribes would still have been

required to expend many man-hours replicating controversial texts and the texts would thus have reached fewer hands.

Just because a technology fits the definition of being disruptive, this does not make it inherently bad. The printing press, perhaps the most disruptive technology of its day, contributed greatly to the advancement of ideas that at the time were considered radical and helped fuel conflicts that would devastate Europe in the middle of the last millennia. When one looks back through history, however, one realizes that the easily replicable process of information distribution also contributed greatly to the spread of scientific knowledge. By making texts cheaply replicable, commoners could now afford to read which in turn increased the demand for education among common people. How much further might human cultural and scientific progress lag behind today if the printing press had not disrupted the legacy network of manuscript production in the 15th century?

Future disruptive technologies will likely have similar negative consequences when they immerge. But they will have positive effects as well. Because of the myriad of beneficial incentives that drive the creation of many of these technologies, it is likely that the beneficial uses of these technologies will grossly outweigh the detrimental ones, just as the uses of the printing press did. It would therefore be a mistake to reflexively move to restrict access to such technologies or otherwise stifle their development because someone might do something undesirable with them.

Furthermore, one must acknowledge that creating mayhem is already an industry with fairly low barriers to entry. Why then do we see relatively little of it in the classically liberal societies of the West? Again, participating in modern society offers the individual a multitude of incentives as compared to the dangerous and uncertain alternatives offered by the use of violence. As long as persons remain relatively free from coercion, history appears to suggest that the rewards of innovation, profit, and self-fulfillment are far more alluring.

Disruptive technologies will push back the bounds of areas in life where coercion and institutional mediation are tolerated. People will likely become ever more powerful agents in the creation of their own worlds [32]. Attempting to interfere in this process

will likely retard human social and technological progress while simultaneously inviting the very backlash that the modern “clergy” of legislators and legacy corporations seem to fear. The need for limited, highly specific, and flexible responses is thus established.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. DATA AND OUTPUT FILE (NON-INTERDICTED LEGACY NETWORK)

```
Decomp finished

OPTIMAL Attack:

OPTIMAL Project ResponseFinish time:     6239.00
 kSTART            0    0.00
 k1                0    0.00
*k2S               0    0.00
 k2F             960    0.00
*k12S              0    0.00
 k12F            960    0.00
 k15S              0    0.00
 k15F            960    0.00
 k16               0    0.00
*k17S              0    0.00
 k17F           2400    0.00
*k22S              0    0.00
 k22F           2400    0.00
 k25S              0    0.00
 k25F           2400    0.00
 k26               0    0.00
*k27S              0    0.00
 k27F           2400    0.00
*k41S              0    0.00
 k41F           2400    0.00
 k42S              0    0.00
 k42F           2400    0.00
 k43               0    0.00
 k44            2400    0.00
 k55            3360    0.00
 k56S              0    0.00
 k56F           4800    0.00
 k57               0    0.00
 k58             960    0.00
 k59            4320    0.00
 k60S           2400    0.00
 k60F           3360    0.00
 k61            2400    0.00
 k62            2880    0.00
 k63               0    0.00
 k64            3360    0.00
 k65            4800    1.00
 k66            6240    1.00
```

k	d	delayy	Yhat	pen_skip
k1	2400	0	0	1
k2S	0	0	0	1
k2F	0	0	0	0
k3S	0	0	0	1
k3F	0	0	0	0
k4	72000	0	0	1
k5	960	0	0	1
k6	3360	0	0	1
k7	960	0	0	1
k8S	0	0	0	1
k8F	0	0	0	0
k9	3360	0	0	1
k10	1440	0	0	1
k11	960	0	0	1
k12S	0	0	0	1
k12F	0	0	0	0
k13S	0	0	0	1
k13F	0	0	0	0
k14	1440	0	1	1
k15S	0	0	0	1
k15F	0	0	0	0
k16	960	0	1	1
k17S	0	0	0	1
k17F	0	0	0	0
k18S	0	0	0	1
k18F	0	0	0	0
k19	2400	0	0	1
k20	2400	0	0	1
k21	1440	0	0	1
k22S	0	0	0	1
k22F	0	0	0	0
k23S	0	0	0	1
k23F	0	0	0	0
k24	3360	0	0	1
k25S	0	0	0	1
k25F	0	0	0	0
k26	2400	0	0	1
k27S	0	0	0	1
k27F	0	0	0	0
k28S	0	0	0	1
k28F	0	0	0	0
k29	3360	0	0	1
k30S	0	0	0	1
k30F	0	0	0	0
k31S	0	0	0	1
k31F	0	0	0	0
k32	1440	0	0	1
k33	0	0	0	1
k34S	0	0	0	1
k34F	0	0	0	0
k35	1440	0	0	1
k36	0	0	0	1
k37S	0	0	0	1
k37F	0	0	0	0
k38	480	0	0	1
k39	960	0	0	1
k40	960	0	0	1
k41S	0	0	0	1
k41F	0	0	0	0
k42S	0	0	0	0
k42F	0	0	0	0
k43	960	0	0	1
k44	0	0	0	0
k45S	0	0	0	0
k45F	0	0	0	0
k46	1440	0	0	1
k47	0	0	0	0
k48S	0	0	0	1
k48F	0	0	0	0
k49	3360	0	0	1
k50	1440	0	0	1
k51S	0	0	0	1
k51F	0	0	0	0
k52	480	0	0	1
k53	960	0	0	1
k54	960	0	0	1
k55	1440	0	0	1
k56S	0	0	0	1
k56F	0	0	0	0
k57	960	0	0	1
k58	1440	0	0	1
k59	480	0	0	1
k60S	0	0	0	1
k60F	0	0	0	0
k61	960	0	0	1
k62	480	0	0	1
k63	1440	0	0	1
k64	1440	0	0	1
k65	1440	1	0	1
k66	480	1	0	1

APPENDIX B. DATA AND OUTPUT FILE (TOTALLY VULNERABLE LEGACY NETWORK)

```
OPTIMAL Attack:
  k64                1.00
  k65                1.00

OPTIMAL Project ResponseFinish time:    66239.00
 kSTART              0     0.00
 k1                  0     0.00
*k2S                 0     0.00
 k2F              1440     0.00
*k12S                0     0.00
 k12F             1440     0.00
 k15S                0     0.00
 k15F             1440     0.00
 k16                 0  1000.00
*k17S                0     0.00
 k17F             2400     0.00
*k22S                0     0.00
 k22F             2400     0.00
 k25S                0     0.00
 k25F             2400     0.00
 k26                 0   300.00
*k27S                0     0.00
 k27F             2400     0.00
*k41S                0     0.00
 k41F             2400     0.00
 k42S                0     0.00
 k42F             2400     0.00
 k43                 0  8000.00
 k44              2400     0.00
 k55             33360     0.00
 k56S                0     0.00
 k56F            34800     0.00
 k57                 0     0.00
 k58               960     0.00
 k59             34320     0.00
 k60S             2400     0.00
 k60F             3360     0.00
 k61              2400     0.00
 k62              2880     0.00
 k63                 0     0.00
 k64              3360     0.00
 k65             34800     0.00
 k66             66240     1.00
```

k	d	delayy	Yhat	pen_skip
k1	2400	0	0	1
k2S	0	0	0	1
k2F	0	0	0	0
k3S	0	0	0	1
k3F	0	0	0	0
k4	72000	0	0	1
k5	960	0	0	1
k6	3360	0	0	1
k7	960	0	0	1
k8S	0	0	0	1
k8F	0	0	0	0
k9	3360	0	0	1
k10	1440	0	0	1
k11	960	0	0	1
k12S	0	0	0	1
k12F	0	0	0	0
k13S	0	0	0	1
k13F	0	0	0	0
k14	2400	2000	1	1
k15S	0	0	0	1
k15F	0	0	0	0
k16	1440	1000	1	1
k17S	0	0	0	1
k17F	0	0	0	0
k18S	0	0	0	1
k18F	0	0	0	0
k19	2400	0	0	1
k20	2400	0	0	1
k21	1440	0	0	1
k22S	0	0	0	1
k22F	0	0	0	0
k23S	0	0	0	1
k23F	0	0	0	0
k24	3360	500	0	1
k25S	0	0	0	1
k25F	0	0	0	0
k26	2400	300	0	1
k27S	0	0	0	1
k27F	0	0	0	0
k28S	0	0	0	1
k28F	0	0	0	0
k29	3360	0	0	1
k30S	0	0	0	1
k30F	0	0	0	0
k31S	0	0	0	1
k31F	0	0	0	0
k32	1440	0	0	1
k33	0	0	0	1
k34S	0	0	0	1
k34F	0	0	0	0
k35	1440	0	0	1
k36	0	0	0	1
k37S	0	0	0	1
k37F	0	0	0	0
k38	480	0	0	1
k39	960	0	0	1
k40	960	0	0	1
k41S	0	0	0	1
k41F	0	0	0	0
k42S	0	0	0	0
k42F	0	0	0	0
k43	1440	8000	1	1
k44	0	0	0	0
k45S	0	0	0	0
k45F	0	0	0	0
k46	2400	9000	1	1
k47	0	0	0	0
k48S	0	0	0	1
k48F	0	0	0	0
k49	3360	1000	1	1
k50	1440	0	0	1
k51S	0	0	0	1
k51F	0	0	0	0
k52	480	0	0	1
k53	960	0	0	1
k54	960	0	0	1
k55	1440	0	0	1
k56S	0	0	0	1
k56F	0	0	0	0
k57	960	0	0	1
k58	1440	0	0	1
k59	480	0	0	1
k60S	0	0	0	1
k60F	0	0	0	0
k61	960	0	0	1
k62	480	0	0	1
k63	1440	0	0	1
k64	1440	30000	0	1
k65	1440	30000	1	1
k66	480	1	1	1

APPENDIX C. OUTPUT FILE AND DATA (FEASIBLE INTERDICTION OF THE LEGACY NETWORK)

```
Decomp finished

OPTIMAL Attack:
  k14                1.00
  k16                1.00
  k43                1.00
  k46                1.00

OPTIMAL Project ResponseFinish time:     7680.00
```

k	d	delayy	Yhat	pen_skip
k1	2400	0	0	1
k2S	0	0	0	1
k2F	0	0	0	0
k3S	0	0	0	1
k3F	0	0	0	0
k4	72000	0	0	1
k5	960	0	0	1
k6	3360	0	0	1
k7	960	0	0	1
k8S	0	0	0	1
k8F	0	0	0	0
k9	3360	0	0	1
k10	1440	0	0	1
k11	960	0	0	1
k12S	0	0	0	1
k12F	0	0	0	0
k13S	0	0	0	1
k13F	0	0	0	0
k14	2400	2000	1	1
k15S	0	0	0	1
k15F	0	0	0	0
k16	1440	1000	1	1
k17S	0	0	0	1
k17F	0	0	0	0
k18S	0	0	0	1
k18F	0	0	0	0
k19	2400	0	0	1
k20	2400	0	0	1
k21	1440	0	0	1
k22S	0	0	0	1
k22F	0	0	0	0
k23S	0	0	0	1
k23F	0	0	0	0
k24	3360	0	0	1
k25S	0	0	0	1
k25F	0	0	0	0
k26	2400	0	0	1
k27S	0	0	0	1
k27F	0	0	0	0
k28S	0	0	0	1
k28F	0	0	0	0
k29	3360	0	0	1
k30S	0	0	0	1
k30F	0	0	0	0
k31S	0	0	0	1
k31F	0	0	0	0
k32	1440	0	0	1
k33	0	0	0	1
k34S	0	0	0	1
k34F	0	0	0	0
k35	1440	0	0	1
k36	0	0	0	1
k37S	0	0	0	1
k37F	0	0	0	0
k38	480	0	0	1
k39	960	0	0	1
k40	960	0	0	1
k41S	0	0	0	1
k41F	0	0	0	0
k42S	0	0	0	0
k42F	0	0	0	0
k43	1440	9000	1	1
k44	0	0	0	0
k45S	0	0	0	0
k45F	0	0	0	0
k46	2400	8000	1	1
k47	0	0	0	0
k48S	0	0	0	1
k48F	0	0	0	0
k49	3360	0	1	1
k50	1440	0	0	1
k51S	0	0	0	1
k51F	0	0	0	0
k52	480	0	0	1
k53	960	0	0	1
k54	960	0	0	1
k55	1440	0	0	1
k56S	0	0	0	1
k56F	0	0	0	0
k57	960	0	0	1
k58	1440	0	0	1
k59	480	0	0	1
k60S	0	0	0	1
k60F	0	0	0	0
k61	960	0	0	1
k62	480	0	0	1
k63	1440	0	0	1
k64	1440	0	0	1
k65	1440	0	1	1
k66	480	0	1	1

APPENDIX D. OUTPUT FILE AND TASK DATA (FEASIBLE INTERDICTION OF THE LEGACY NETWORK II)

```
OPTIMAL Attack:
  k14                1.00
  k16                1.00
  k43                1.00
  k46                1.00
  k49                1.00

OPTIMAL Project ResponseFinish time:     8639.00
```

k	d	delayy	Yhat	pen_skip
k1	2400	0	0	1
k2S	0	0	0	1
k2F	0	0	0	0
k3S	0	0	0	1
k3F	0	0	0	0
k4	72000	0	0	1
k5	960	0	0	1
k6	3360	0	0	1
k7	960	0	0	1
k8S	0	0	0	1
k8F	0	0	0	0
k9	3360	0	0	1
k10	1440	0	0	1
k11	960	0	0	1
k12S	0	0	0	1
k12F	0	0	0	0
k13S	0	0	0	1
k13F	0	0	0	0
k14	2400	2000	1	1
k15S	0	0	0	1
k15F	0	0	0	0
k16	1440	2000	1	1
k17S	0	0	0	1
k17F	0	0	0	0
k18S	0	0	0	1
k18F	0	0	0	0
k19	2400	0	0	1
k20	2400	0	0	1
k21	1440	0	0	1
k22S	0	0	0	1
k22F	0	0	0	0
k23S	0	0	0	1
k23F	0	0	0	0
k24	3360	0	0	1
k25S	0	0	0	1
k25F	0	0	0	0
k26	2400	0	0	1
k27S	0	0	0	1
k27F	0	0	0	0
k28S	0	0	0	1
k28F	0	0	0	0
k29	4800	0	0	1
k30S	0	0	0	1
k30F	0	0	0	0
k31S	0	0	0	1
k31F	0	0	0	0
k32	1440	0	0	1
k33	0	0	0	1
k34S	0	0	0	1
k34F	0	0	0	0
k35	1440	0	0	1
k36	0	0	0	1
k37S	0	0	0	1
k37F	0	0	0	0
k38	480	0	0	1
k39	960	0	0	1
k40	960	0	0	1
k41S	0	0	0	1
k41F	0	0	0	0
k42S	0	0	0	0
k42F	0	0	0	0
k43	1440	9000	1	1
k44	0	0	0	0
k45S	0	0	0	0
k45F	0	0	0	0
k46	2400	8000	1	1
k47	0	0	0	0
k48S	0	0	0	1
k48F	0	0	0	0
k49	3360	5000	1	1
k50	1440	0	0	1
k51S	0	0	0	1
k51F	0	0	0	0
k52	480	0	0	1
k53	960	0	0	1
k54	960	0	0	1
k55	1440	0	0	1
k56S	0	0	0	1
k56F	0	0	0	0
k57	960	0	0	1
k58	1440	0	0	1
k59	480	0	0	1
k60S	0	0	0	1
k60F	0	0	0	0
k61	960	0	0	1
k62	480	0	0	1
k63	1440	0	0	1
k64	1440	0	0	1
k65	1440	1	1	1
k66	480	1	1	1

APPENDIX E. OUTPUT FILE AND TASK DATA (NON-INTERDICTED ADVANCED NETWORK)

```
DISTECH project management 16.03.23
Decomp finished

OPTIMAL Attack:

OPTIMAL Project ResponseFinish time:     2880.00
 kSTART                0.00
 k1                    0.00
*k2S                 480.00
 k3S                 480.00
 k4                 1440.00
 k5                 1440.00
 k6                  480.00
 k7                  960.00
 k8                 1440.00
*k15S                 0.00
 k16S                 0.00
 k17                2400.00
 k18                2880.00
 k22                1440.00
 k23                1440.00
 k24                1920.00
 k25                2880.00
```

k	d	delayy	Yhat	pen_skip
k1	480	0	0	0
k2S	0	0	0	0
k2F	0	0	0	0
k3S	0	0	0	0
k3F	0	0	0	0
k4	480	0	0	0
k5	480	0	0	0
k6	480	0	0	0
k7	480	0	0	0
k8	960	0	0	0
k9S	0	0	0	0
k9F	0	0	0	0
k10	480	0	0	0
k11	480	0	0	0
k12	1440	0	0	0
k13	480	0	0	0
k14	960	0	0	1
k15S	0	0	0	0
k15F	0	0	0	0
k16S	0	0	0	0
k16F	0	0	0	0
k17	480	0	0	0
k18	480	0	0	0
k19S	0	0	0	0
k19F	0	0	0	0
k20	480	0	0	0
k21	1440	0	0	0
k22	480	0	0	0
k23	480	0	0	0
k24	960	0	0	0
k25	960	0	0	0

APPENDIX F. OUTPUT FILE AND TASK DATA (TOTALLY VULNERABLE ADVANCED NETWORK)

```
OPTIMAL Attack:
  k24                1.00
  k25                1.00

OPTIMAL Project ResponseFinish time:     22880.00
 kSTART              0     0.00
*k1S                 0     0.00
 k1F              1440     0.00
 k2S                 0     0.00
 k2F              1440     0.00
 k3                960     0.00
 k4                960     0.00
 k5                960     0.00
 k6                  0     0.00
 k7                480     0.00
 k8                960     0.00
*k15S                0     0.00
 k15F            12400     0.00
 k16S                0     0.00
 k16F            12400     0.00
 k17                 0     0.00
 k18             11920     0.00
 k22              1440     0.00
 k23              1440     0.00
 k24              1920     0.00
 k25             12400     0.00
 k26             22880     0.00
```

k	d	delayy	Yhat	pen_skip
k1S	0	0	0	1
k1F	0	0	0	0
k2S	0	0	0	1
k2F	0	0	0	0
k3	480	0	0	1
k4	480	0	0	1
k5	480	0	0	1
k6	480	0	0	1
k7	480	0	0	1
k8	480	0	0	1
k9S	0	0	0	1
k9F	0	0	0	0
k10	480	0	0	1
k11	480	0	0	1
k12	960	0	0	1
k13	480	0	0	1
k14	480	0	0	1
k15S	0	0	0	1
k15F	0	0	0	0
k16S	0	0	0	1
k16F	0	0	0	0
k17	480	0	0	1
k18	480	0	0	1
k19S	0	0	0	1
k19F	0	0	0	0
k20	480	0	0	1
k21	960	0	0	1
k22	480	0	0	1
k23	480	0	0	1
k24	480	10000	0	1
k25	480	10000	0	1
k26	480	0	0	1

APPENDIX G. OUTPUT FILE AND TASK DATA (FEASIBLE INTERDICTION ON ADVANCED NETWORK)

```
OPTIMAL Attack:
  k5                1.00

OPTIMAL Project ResponseFinish time:     3840.00
 kSTART             0    0.00
*k1S                0    0.00
 k1F             2400    0.00
 k9S                0    0.00
 k9F             2400    0.00
 k10             1920    0.00
 k11                0    0.00
 k12              480    0.00
 k13             1440    0.00
 k14             1920    0.00
*k15S               0    0.00
 k15F            3360    0.00
 k16S               0    0.00
 k16F            3360    0.00
 k17                0    0.00
 k18             2880    0.00
 k22             2400    0.00
 k23             2400    0.00
 k24             2880    0.00
 k25             3360    0.00
 k26             3840    0.00
```

k	d	delayy	Yhat	pen_skip
k1S	0	0	0	1
k1F	0	0	0	0
k2S	0	0	0	1
k2F	0	0	0	0
k3	480	0	0	1
k4	480	0	0	1
k5	480	10000	0	1
k6	480	0	0	1
k7	480	0	0	1
k8	480	0	0	1
k9S	0	0	0	1
k9F	0	0	0	0
k10	480	0	0	1
k11	480	0	0	1
k12	960	0	0	1
k13	480	0	0	1
k14	480	0	0	1
k15S	0	0	0	1
k15F	0	0	0	0
k16S	0	0	0	1
k16F	0	0	0	0
k17	480	0	0	1
k18	480	0	0	1
k19S	0	0	0	1
k19F	0	0	0	0
k20	480	0	0	1
k21	960	0	0	1
k22	480	0	0	1
k23	480	0	0	1
k24	480	0	0	1
k25	480	0	0	1
k26	480	0	0	1

LIST OF REFERENCES

[1] J. W. Peters, D. J. Tanner, and A. Kasper, *Explosives and Blasting.* Eugene, OR: Do North Media, 2010.

[2] T. Krainin. (2014, Apr. 18). Cody Wilson: Happiness is a 3-D printed gun [Online]. Available: http://reason.com/reasontv/2014/04/18/cody-wilson-happiness-is-a-3-d-printed-g. Accessed Apr. 18, 2014.

[3] E. Lorain. (2010, Dec. 10). Cody Wilson philosophy part I. [YouTube video]. Available: https://www.youtube.com/watch?v=v3zx8kyVtGM. Accessed Feb., 2013.

[4] A. Greenberg. (2015, May 7). 3-D printed gun lawsuit starts the war between arms control and free speech. [Online]. Available: https://www.wired.com/2015/05/3-d-printed-gun-lawsuit-starts-war-arms-control-free-speech/. Accessed May 8, 2015.

[5] M. Burke. (2016, May 10). What are molecular prosthetics? [Online]. Available: http://benefunder.org/causes/461/marty-burke). Accessed Aug. 5, 2016.

[6] M. Burke et al. "Apparatus and methods for the automated synthesis of small molecules," U.S. Patent 2011/045064, May 29, 2013.

[7] Carnegie Mellon researchers hack off-the-shelf 3-D printer to rebuild human heart. (2015, Oct. 23). [Online]. Available: https://engineering.cmu.edu/media/feature/2015/10_23_feinberg_paper.html. Accessed Jan. 4, 2016.

[8] A. Peterson. (2015, Sep. 10). The 'Crypto Wars' of the 1990s are brewing again in Washington. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2015/09/10/the-crypto-wars-of-the-1990s-are-brewing-again-in-washington/. Accessed Sep. 12, 2015.

[9] N. Perlroth. (2015, Jul. 8). Security experts oppose government access to encrypted communication. [Online]. Available: http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?_r=0. Accessed June 4, 2016.

[10] D. Shamah. (2016, Apr. 4). Gov't contract a strong sign FBI used Israeli tech to crack San Bernadino iPhone. [Online]. Available: http://www.timesofisrael.com/fbi-contract-a-strong-sign-fbi-used-israeli-tech-to-crack-san-bernardino-iphone/. Accessed May 27, 2016.

[11] P. Sayer. (2014, Dec. 29). Snowden docs show Tor, TrueCrypt, Tails topped NSA's 'most wanted' list in '12. [Online]. Available: http://www.computerworld.com/article/2863937/snowden-docs-show-tor-truecrypt-tails-topped-nsas-most-wanted-list-in-12.html . Accessed May 27, 2016.

[12] M. Lee. (2015, Nov. 12) Edward Snowden explains how to reclaim your privacy. [Online]. Available: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/. Accessed May 27, 2016.

[13] S. Nelson. (2015, Sept. 2). Buying drugs online remains easy, 2 years after FBI killed Silk Road. [Online]. Available: http://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road. Accessed June 2, 2016.

[14] M. Farrell. (2013, Mar. 28). Bitcoin prices surge post-Cyprus bailout. [Online]. Available: http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/. Accessed Mar. 28, 2013.

[15] A. Liu. (2013, Mar. 19). When governments take your money, Bitcoin looks really good. [Online]. Available: http://motherboard.vice.com/blog/cyprus-spain-when-governments-take-your-money-bitcoin-looks-really-good. Accessed Aug 15, 2016.

[16] J. Epstein. (2016, Mar. 18). Can Ethereum restore online freedom and transform the Internet. [Online]. Available: http://reason.com/reasontv/2016/03/18/ethereum-blockchain-lubin-consensys. Accessed Mar. 18, 2016.

[17] G. G. Brown, W. M. Carlyle, R. C. Harney, E. Skroch, and R. K. Wood, "Anatomy of a project to produce a first nuclear weapon," *Science and Global Security*, vol. 14, pp. 163–182, 2006.

[18] G. G. Brown, W. M. Carlyle, J. Royset, and K. Wood, *On the Complexity of Delaying an Adversary's Project.* Monterey, CA: NPS Faculty Publications, 2005.

[19] E. Skroch, "How to optimally interdict a belligerent project to develop a nuclear weapon," MS thesis, Dept. of Operations Research, Naval Postgraduate School, Monterey, CA, 2004.

[20] G.G. Brown, W.M. Carlyle, R.C. Harney, E. Skroch, R.K. Wood, "Interdicting a nuclear-weapons project," *Operations Research*, vol. 57, pp. 866–877, 2009.

[21] P. Nesbitt, 2012, "Delaying a nuclear proliferator: Interdicting combined social network and project management models," MS thesis, Dept. of Operations Research, Naval Postgraduate School, Monterey, CA, 2012.

[22] E. Davis, J. E. Moder, and C. Phillips, *Project Management with CPM, PERT, and Precedence Diagramming*. New York, NY: Van Nostrand Reinhold, 1983.

[23] Project Professional 2010, version 2010, Microsoft Corporation, Redmond, WA, 2010.

[24] *Improvised Munitions Manual*, TM 31–210, U.S. Department of the Army, Washington, DC, 1969.

[25] D. L. Alderson, G. G. Brown, and W. M. Carlyle, "Assessing and Improving Operational Resilience of Critical Infrastructures and other Systems," *Tutorials in Operations Research, INFORMS*, pp. 180–215, 2014.

[26] July 7 2005 London bombing fast facts. (2013, Nov. 6). [Online]. Available: http://www.cnn.com/2013/11/06/world/europe/july-7-2005-london-bombings-fast-facts/. Accessed Aug 16, 2016.

[27] N. C. Asthana and A. Nirmal, *The Ultimate Book of Explosives, Bombs and IEDs*. Jaipur (Raj), India: Pointer Publishers, 2008.

[28] R. Turkington, *Chemicals Used For Illegal Purposes*. Hoboken, New Jersey, John Wiley & Sons, 2010.

[29] J.D. Tuccille.(2016, May 17). Print your own drugs, for health and fun. [Online]. Available: http://reason.com/archives/2016/05/17/print-your-own-drugs-for-health-and-fun. Accessed May 17, 2016.

[30] W. J. Broad, J. Markoff, and D. Sanger. (2011, Jan. 15). Israeli test on worm called crucial in Iran nuclear delay. [Online]. Available: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0. Accessed May 26, 2016.

[31] Thomson Reuters,(2011, Apr. 25). Stars' virus detected by Iran in second cyber war attempt. [Online]. Available: http://www.huffingtonpost.com/2011/04/25/stars-virus-iran-cyber-attack_n_853219.html. Accessed May 26, 2016.

[32] C. Wilson. *Come and Take It: The Gun Printer's Guide to Thinking Free*, New York, NY: Gallery Books, An Imprint of Simon and Schuster, 2016.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California